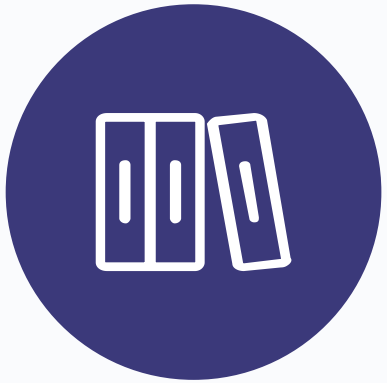


第3章 数据安全防护架构

成都信息工程大学 白杨 Alicepub@163.com

2024年11月4日

第3章 数据安全防护架构

本讲内容概要：

01 第一节—数据全生命周期安全

02 第二节—数据采集安全

03 第三节—数据存储安全

04 第四节—数据使用安全

05 第五节—数据加工安全

第3章 数据安全防护架构

本讲内容概要：

06 第六节—数据传输安全

07 第七节—数据提供安全

08 第八节—数据公开安全

09 第九节—数据销毁安全

01 1.1 数据全生命周期安全

数据全生命周期安全体系

01 1.1 数据全生命周期安全

（1）数据安全治理

- **数据安全规划**

要确定组织数据安全治理工作的总体定位和愿景，根据组织整体发展战略内容，结合实际情况进行现状分析，制定数据安全规划，并对规划进行充分论证。

- **数据安全建设**

对数据安全规划进行落地实施，建成与组织相适应的数据安全治理能力，包括组织架构建设、制度体系完善、技术工具建立和人员能力培养等。

- **数据安全运营**

不断适配业务环境和风险管理需求，持续优化安全策略措施，强化整个数据安全治理体系的有效运转。

- **数据安全评估优化**

通过内部评估与第三方评估相结合的方式，对组织的数据安全治理能力进行评估分析，总结不足并动态纠偏，实现数据安全治理的持续优化及闭环工作机制的建立。

01 1.1 数据全生命周期安全

（2）数据安全分级防护

数据安全分级防护是基于数据生命周期各个阶段的精细化安全策略。为了确保数据在生命周期的不同阶段都得到适当的保护，数据安全分级防护提出了针对性的安全防护策略。

- **数据采集安全**：数据源可信、数据内容合规、数据完整性、数据真实性、数据采集安全管理
- **数据存储安全**：数据存储合规、数据存储安全、存储完整性、数据时效性
- **数据使用安全**：数据导入导出安全、数据分析安全、数据确权、数据处理环境安全
- **数据加工安全**：细粒度访问控制
- **数据传输安全**：数据传输机密性、数据传输完整性
- **数据提供安全**：数据安全溯源、数据导入/导出安全、接口安全
- **数据公开安全**：导入/导出安全、接口安全
- **数据销毁安全**：安全销毁

01 1.1 数据全生命周期安全

（3）数据安全防护技术

数据安全防护技术涵盖了数据加密、数据脱敏、数据访问控制、数据水印、数据容灾备份、数据安全销毁、隐私计算、数据审计、数据安全治理共 9 个部分。

- **数据加密**：使用加密算法和密钥管理技术，确保数据在传输和存储过程中不会被未授权访问或篡改
- **数据脱敏**：对敏感数据进行脱敏处理，即在保留数据格式的同时去除或替换其中的敏感信息
- **数据访问控制**：对用户身份进行验证和授权，确保只有合法用户能够访问和操作数据
- **数据水印**：在数据中添加特定的标记信息，可以追溯数据的来源
- **数据容灾备份**：数据容灾是为了在遭遇灾害时能保证信息系统能正常运行，数据备份是为了应对灾难来临时造成的数据丢失问题。
- **数据安全销毁**：针对数据的内容进行清除和净化
- **隐私计算**：保证数据提供方不泄露原始数据的前提下，对数据进行分析计算
- **数据审计**：对数据进行采集、转换、清理、验证和分析
- **数据安全治理**：制定数据安全策略，对数据分级分类，对数据的全生命周期进行管理

01 1.1 数据全生命周期安全

（4）数据分类分级

数据分类分级对于数据基础制度建设具有重要意义，不仅是完善数据产权、规范数据交易的前提条件，也是维护数据安全的必要手段。

相关法律政策和标准规范：

- 《网络安全法》
- 《数据安全法》
- 《个人信息保护法》
- 《网络数据安全管理条例（征求意见稿）》
- 《工业数据分类分级指南（试行）》
- ……

01 1.1 数据全生命周期安全

（5）数据安全标准规范

在对数据进行安全防护的同时，也需要遵守相应的数据安全标准规范。当前，已有许多政府或企业等官方机构出台了数据安全的标准规范，此处列举几项以供参考。

- 《GB/T 37973-2019 信息安全技术大数据安全管理指南》
- 《数据安全治理白皮书 5.0》
- 《GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型》
- 国家标准《信息安全技术 数据安全风险评估方法（征求意见稿）》
- .....

01 1.1 数据全生命周期安全

数据全生命周期安全体系的意义

- **保护隐私和个人信息安全**
- **维护商业机密和竞争优势**
- **确保数据的准确性和完整性**
- **遵守法规和合规性要求**
- **增强信任和声誉**
- **降低安全风险和成本**

第3章 数据安全防护架构

本讲内容概要：

01 第一节—数据全生命周期安全

02 第二节—数据采集安全

03 第三节—数据存储安全

04 第四节—数据使用安全

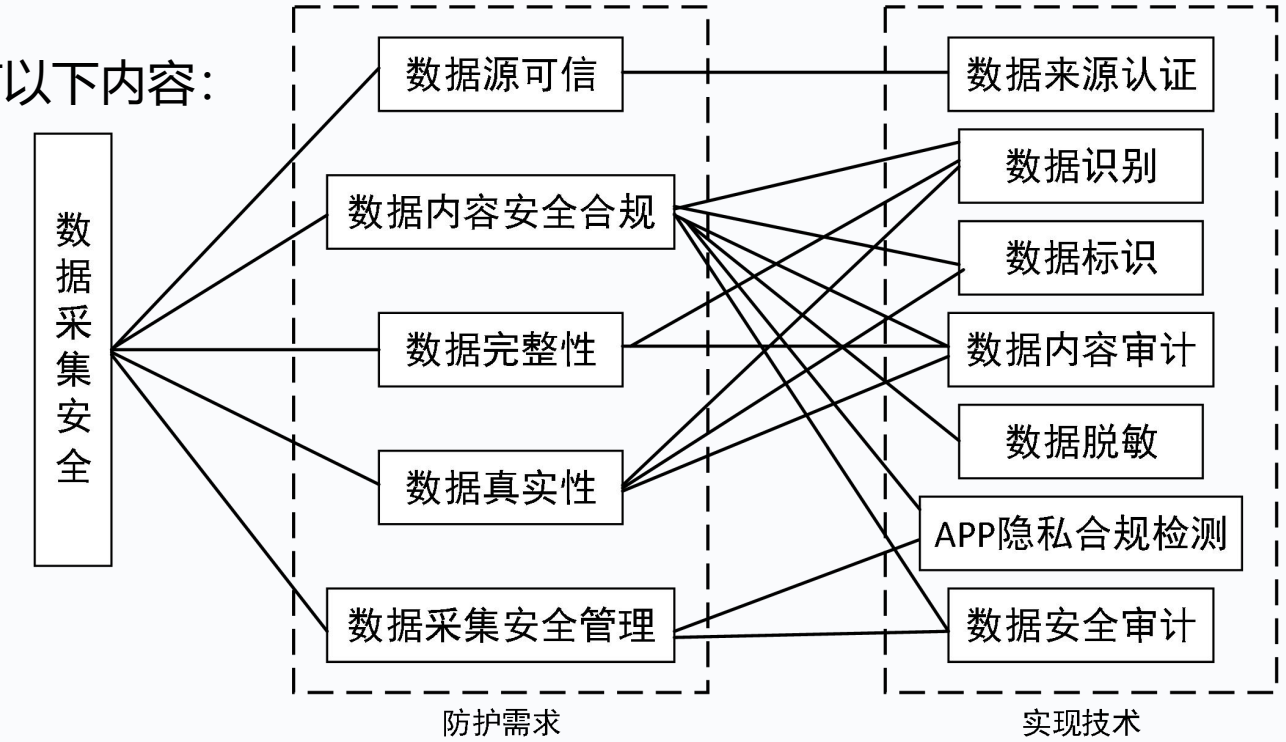
05 第五节—数据加工安全

02 2.1 数据采集安全

数据采集安全是指根据组织对数据采集的安全要求，建立数据采集安全管理措施和安全防护措施，规范数据采集相关的流程，从而保证数据采集的合法、合规、正当和诚信。

通常数据采集安全防护需求包含有以下内容：

- **数据源可信**
- **数据内容安全合规**
- **数据完整性**
- **数据真实性**
- **数据采集安全管理**



02 2.1 数据采集安全

数据源可信

数据采集安全首要考虑的应当是数据源的安全问题。对数据采集来源进行管理的目的是确保采集数据的数据源是安全可信的，确保采集对象是可靠的。采集数据源的安全可通过数据源可信认证技术来实现，包括可信管理、身份鉴定、用户授权等。

数据来源认证，可分为数据源鉴别和数据源记录两部分：

- 数据源鉴别：对收集的数据源进行身份识别，以防止组织机构采集到其他非法或不被认可的数据源产生的数据，防止采集到错误的或失真的数据
- 数据源记录：对需要提供数据采集服务的数据源进行标识与记录，保证可以在必要时对数据源进行追踪和溯源。

02 2.1 数据采集安全

数据内容安全合规

针对数据内容安全合规，通常使用**数据识别、数据标识、数据内容审计、数据脱敏、APP隐私合规检测和数据安全审计技术**来确保采集的数据符合各项法规制度和要求。

- 数据识别技术通过对数据进行分类和识别，帮助确定哪些数据是敏感数据，从而为数据保护和合规性检测提供基础。
- 数据标识则通过对数据进行标签化，明确标识其敏感性等级和使用权限，确保合规要求得到遵守。数据内容审计通过实时监控和记录数据操作行为，及时发现数据访问和处理过程中的异常情况，保证操作的合法性和合规性。
- 数据脱敏技术可以在保留数据的可用性同时，降低数据泄露风险。
- APP隐私合规检测通过分析应用程序的数据收集、存储、使用和共享行为，避免数据滥用和泄露。
- 数据安全审计技术能对数据处理和访问全过程进行全程监控和审计，确保每一个环节符合合规性要求，并提供合规性报告，减少法律和安全风险。

02 2.1 数据采集安全

数据内容安全合规

- **个人信息保护**

  相关法规：《网络安全法》、《民法总则》、《民法典》、《个人信息保护法》、《数据安全法》

- **重要数据保护**

  重要数据的定义：特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。

  保护：《数据安全法》针对重要数据规定了重要数据目录制定、数据安全审查和数据出口管制等制度。

- **数据跨境传输**

  数据跨境含义：“数据从一法域被转移至另一法域的行为”或“跨越国界对存储在计算机中的机器可读数据进行处理”。

  相关法规：《数据安全法》、《个人信息保护法》、《数据安全出境评估办法》（征求意见稿）、《网络数据安全管理条例》（征求意见稿）、《网络安全审查办法》（征求意见稿）

02 2.1 数据采集安全

数据完整性

数据完整性的一个主要目标是防止数据在传输或存储过程中被未经授权的篡改。通过数据完整性保护机制，如**加密、数字签名**等技术，可以检测到数据是否被篡改，并在发现篡改时及时做出响应，保证数据的完整性。利用数据识别技术，准确识别和分类不同类型的数据，为数据完整性的保护提供了基础。此外，还可以通过数据内容审计技术，进一步检验数据采集过程中的内容完整性和合规性。

数据真实性

通过建立真实数据规则库以及采用数据内容审计技术来检验数据的真实性。针对涉及个人隐私的信息，可以采用数据脱敏技术进行处理。

采用的防护技术包括：**数据标识、数据识别、数据内容审计**

02 2.1 数据采集安全

数据采集安全管理

数据采集安全管理，在《GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型》中描述定义为在采集外部客户、合作伙伴等相关方数据的过程中，组织应明确采集数据的目的和用途，确保满足数据源的真实性、有效性和最少够用等原则要求，并明确数据采集渠道、规范数据格式以及相关的流程和方式，从而保证数据采集的合规性、正当性、一致性。

采用技术：**APP 隐私合规检测、数据安全审计**

第3章 数据安全防护架构

本讲内容概要：

01 第一节—数据全生命周期安全

02 第二节—数据采集安全

03 第三节—数据存储安全

04 第四节—数据使用安全

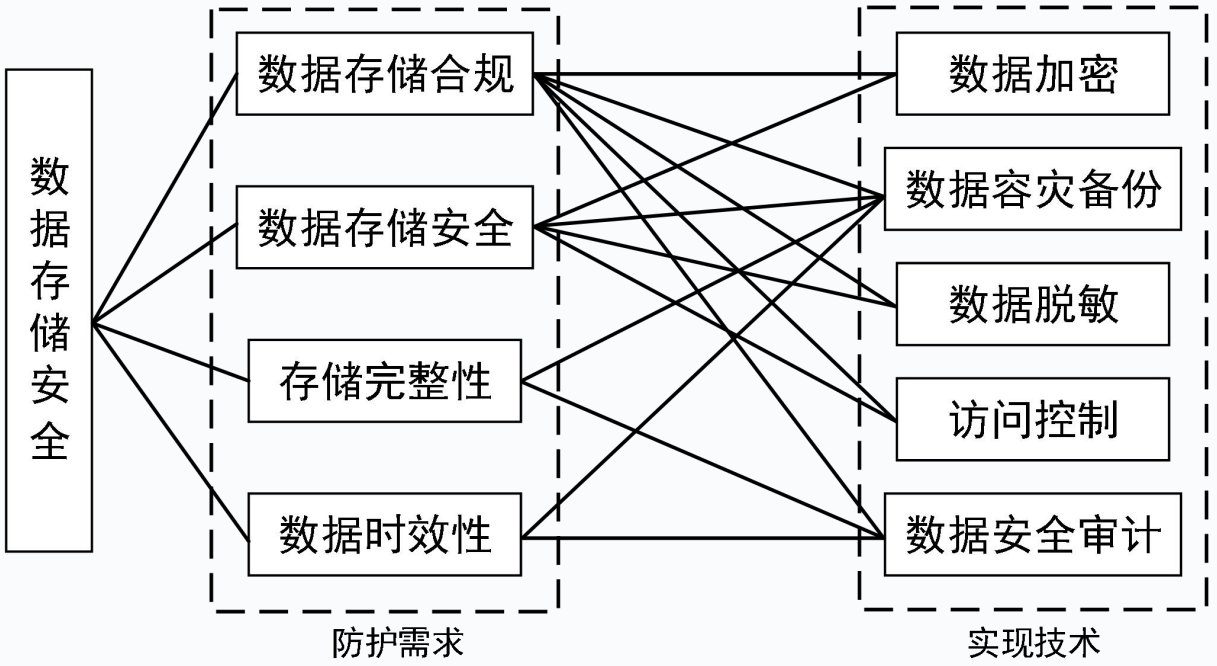
05 第五节—数据加工安全

03 3.1 数据存储安全

数据存储安全是指根据组织内部数据存储安全要求，提供有效的技术和管理手段，防止对存储介质的不当使用而可能引发的数据泄露风险，并规范数据存储的冗余管理流程，保障数据可用性，实现数据存储安全。

通常数据存储安全有以下内容：

- **数据存储合规**
- **数据存储安全**
- **存储完整性**
- **数据时效性**



03 3.1 数据存储安全

数据存储合规

- **存储期限**

  不同的法律法规及文件针对存储时间有着不同的规定，这些规定往往基于不同的行业标准、数据类型和法律要求。如：《个人信息保护法》第 19 条中提到，除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

- **存储范围**

  收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息，存储数据的范围应当为实现目的的最小范围。

  采用的防护技术包含：数据加密、容灾备份、数据脱敏、访问控制、数据安全审计。

03 3.1 数据存储安全

数据存储安全

数据存储安全可以确保个人和敏感信息的保密性，例如使用数据加密和数据脱敏技术对数据的完整性和隐私提供保障。

技术：数据加密、容灾备份、数据脱敏、访问控制

存储完整性

存储完整性指的是数据在存储过程中保持完整、不被篡改或损坏的状态。这种完整性的保证对于数据的可信度、可靠性和可用性至关重要。

技术：数据容灾备份、分析审计日志等

数据时效性

数据时效性是指数据在不同的时间具有很大的性质上的差异，这个差异性定义为数据时效性，时效性影响着数据质量，随着时间的推移，数据质量会快速的下降。

技术：数据容灾备份、分析审计日志等

第3章 数据安全防护架构

本讲内容概要：

01 第一节—数据全生命周期安全

02 第二节—数据采集安全

03 第三节—数据存储安全

04 第四节—数据使用安全

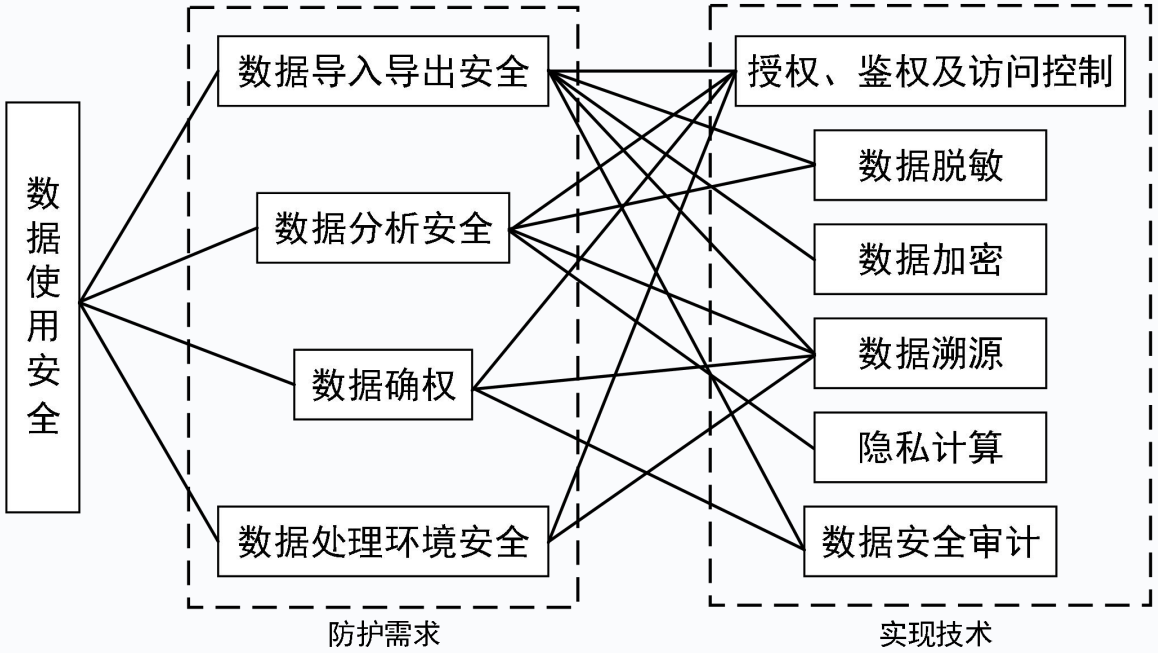
05 第五节—数据加工安全

04 4.1 数据使用安全

数据使用安全指通过数据分析和数据可视化等技术从数据中提取信息，提炼出有用知识和价值的系列操作。在数据使用环节，风险威胁来自于外部因素、内部因素、系统安全等。

通常数据使用安全有以下项：

- **数据导入导出安全**
- **数据分析安全**
- **数据确权**
- **数据处理环境安全**



04 4.1 数据使用安全

数据导入导出安全

数据导入导出是数据交换过程中的重要步骤，因为在数据交换的过程中存在着大量数据导入导出的场景及需求。

数据导入导出安全的技术工具应从两个方面来设计：

- **数据导入安全**，其作用是防止导入恶意数据，造成数据被篡改或破坏；
- **数据导出安全**，其作用是防止导出未授权的数据，造成敏感信息泄露。

数据导入导出安全的全流程必须包含以下几个技术：

授权、鉴权及访问控制；数据脱敏；数据加密；数据溯源；数据安全审计。

04 4.1 数据使用安全

数据分析安全

数据分析安全是通过在数据分析过程采取适当的安全控制措施，防止数据挖掘、分析过程中有价值信息和个人隐私泄漏的安全风险。

技术：访问控制、数据脱敏、数据溯源、隐私计算等

数据确权

数据确权是通过对数据处理者等赋权，使其对数据享有相应的法律控制手段，从而在一定程度或范围内针对数据具有排除他人侵害的效力。数据确权有利于激励数据生产，有利于促进数据流通，有利于解决“数据孤岛”困境。

技术：授权、鉴权、访问控制、数据溯源和数据安全审计技术等

04 4.1 数据使用安全

数据处理环境安全

数据处理环境安全是指如何有效地防止数据损坏，丢失或泄密等问题，比如：数据在录入，处理，统计或打印的过程中，由于硬件故障，断电，死机，人为的误操作，程序缺陷，病毒等造成的数据库损坏或数据丢失问题，以及某些敏感或保密的数据可能会被不具备资格的人员操作或读取，从而造成数据泄密的问题。

技术：访问控制、数据溯源

数据加工安全

数据加工是指对原始数据进行清洗、转换、整合等操作，以便于进行后续的数据分析和挖掘。数据加工的主要目标是将原始数据转换为有价值的信息，以满足企业或个人的需求。泄露风险主要是由分类分级不当、数据脱敏质量较低、恶意篡改/误操作等情况所导致。

主要从加工数据机密性、数据免遭泄露和滥用、细粒度访问控制方面进行。

04 4.1 数据使用安全

数据处理环境安全

数据处理环境安全是指如何有效地防止数据损坏，丢失或泄密等问题，比如：数据在录入，处理，统计或打印的过程中，由于硬件故障，断电，死机，人为的误操作，程序缺陷，病毒等造成的数据库损坏或数据丢失问题，以及某些敏感或保密的数据可能会被不具备资格的人员操作或读取，从而造成数据泄密的问题。

技术：访问控制、数据溯源

第3章 数据安全防护架构

本讲内容概要：

01 第一节—数据全生命周期安全

02 第二节—数据采集安全

03 第三节—数据存储安全

04 第四节—数据使用安全

05 第五节—数据加工安全

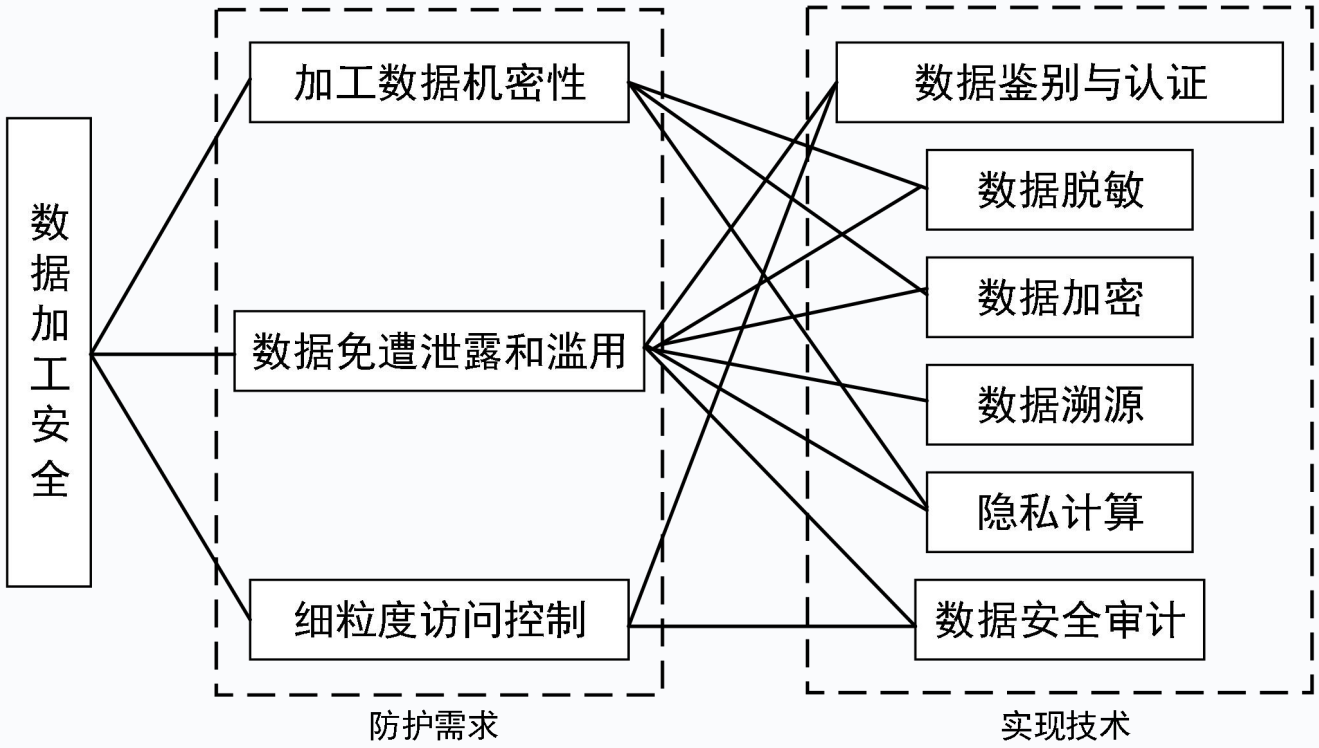
05 5.1 数据加工安全

数据加工是指对原始数据进行清洗、转换、整合等操作，以便于进行后续的数据分析和挖掘。数据加工的主要目标是将原始数据转换为有价值的信息，以满足企业或个人的需求。在数据加工环节，泄露风险主要是由分类分级不当、数据脱敏质量较低、恶意篡改/误操作等情况所导致。

数据加工包括但不限于数据清洗、数据转换、数据整合、数据质量检查等

通常数据加工安全有以下项：

- **加工数据机密性**
- **数据免遭泄露和滥用**
- **细粒度访问控制**



05 5.1 数据加工安全

加工数据机密性

加工数据机密性要求采取严格的防护措施，确保敏感信息在清洗、整合、转换和分析等各个环节不被未授权访问或泄露。

技术：数据加密、数据脱敏、隐私计算，同时，还需关注加工环境的物理安全和网络安全

数据免遭泄露和滥用

在数据加工过程中，面临着诸多潜在的安全威胁，包括数据泄露、不当访问、数据滥用等风险。同时，敏感信息可能因网络攻击、内部人员失误等原因泄露给未经授权的第三方。

技术：数据鉴别与认证、数据溯源、隐私计算、数据安全审计

05 5.1 数据加工安全

细粒度访问控制

在数据加工过程中，由于数据会经过多个不同权限用户的处理，如数据录入员、数据分析师、数据科学家以及管理层等，每个角色对数据的访问和操作需求各不相同。为了确保数据的安全性和完整性，需要使用更加细粒度的访问控制策略来进行权限管控。

细粒度访问控制是基于对单个数据资源的多个条件和/或多个权限来授予或拒绝对关键资产（如资源和数据）的访问的能力。

第3章 数据安全防护架构

本讲内容概要：

06 第六节—数据传输安全

07 第七节—数据提供安全

08 第八节—数据公开安全

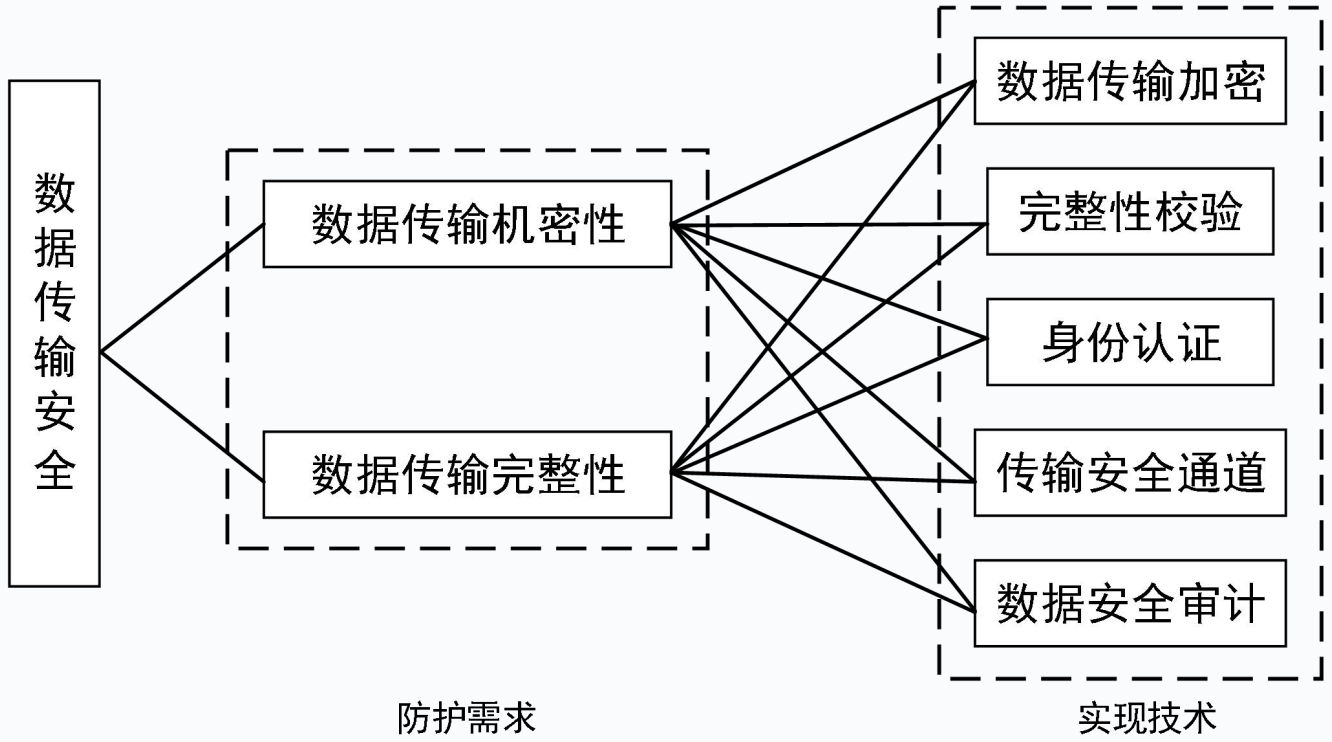
09 第九节—数据销毁安全

06 6.1 数据传输安全

数据传输安全指通过采取必要措施，确保数据在传输阶段，处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。在数据传输环节，会遇到网络攻击、传输泄露等风险。

通常数据传输安全有以下项：

- **数据传输机密性**
- **数据传输完整性**



06 6.1 数据传输安全

数据传输机密性

数据传输活动的“主体”涉及到发送方、接收方以及传输路径上的多个中间节点等多个实体。这些实体共同构成了数据传输的安全责任主体。

数据传输机密性指的是数据在传输过程中必须得到保护，防止被未授权的第三方访问。

数据传输完整性

数据的完整性要求保证数据在传输过程中不被篡改或损坏，确保接收方接收到的数据与发送方发送的数据完全一致。对于数据传输的机密性和完整性，在进行安全防护时并没有特别明显的区分，往往是两者同时进行保护。

技术：数据传输加密、采用完整性校验技术、身份认证、传输安全通道、数据安全审计

第3章 数据安全防护架构

本讲内容概要：

06 第六节—数据传输安全

07 第七节—数据提供安全

08 第八节—数据公开安全

09 第九节—数据销毁安全

07 7.1 数据提供安全

在数据提供环节，风险威胁来自不合规地提供和共享；缺乏数据拷贝的使用管控和终端审计、行为抵赖、数据发送错误、非授权隐私泄露/修改、第三方过失而造成数据泄露；恶意程序入侵、病毒侵扰、网络宽带被盗用等情况。

通常数据提供安全有以下项：

- **数据安全溯源**
- **数据导入/导出安全**
- **接口安全**

07 7.1 数据提供安全

数据安全溯源

数据安全溯源通过先进的数据标识和数据水印技术可精准定位泄露源头，对责任人形成巨大震慑作用的同时，进一步减少违规拍摄、复印等行为的发生，最大化的有效降低数据泄露风险。

技术：

（1）数据标识技术，以规范化的数据格式描述数据属性，采用密码技术对描述信息进行安全保护，能够确保信息完整有效和真实可信。

（2）数据水印是将特定的数字信号嵌入数字产品中保护数字产品版权、完整性、防复制或去向追踪的技术。

07 7.1 数据提供安全

数据导入/导出安全

通过数据导入导出，数据被批量化流转，加速数据应用价值的体现。如果没有安全保障措施，非法人员可能通过非法技术手段导出非授权数据，导入恶意数据等，带来数据篡改和数据泄漏的重大事故，由于一般数据导入导出的数据量都很大，因此相关安全风险和安全危害也会被乘倍放大。

技术：数据脱敏、数据加密、数据安全审计技术

接口安全

随着 API 等数据接口的应用范围急剧增长，由于对其安全保障措施和监测预警机制不足，导致大规模数据泄露等安全事件频出。开展数据接口安全风险监测是避免数据遭受泄露、篡改、滥用等的重要举措。

技术：接口鉴权和接口访问控制技术

第3章 数据安全防护架构

本讲内容概要：

06 第六节—数据传输安全

07 第七节—数据提供安全

08 第八节—数据公开安全

09 第九节—数据销毁安全

08 8.1 数据公开安全

在一般数据全生命周期安全保护中，要求公开前需对其数据进行分析研判，判断是否可公开、是否需脱敏等。在数据公开环节，风险主要是很多数据在未经过严格保密审查、未进行泄密隐患风险评估，或者未意识到数据情报价值或涉及公民隐私的情况下随意发布的情况。

通常数据公开安全有以下项：

- **导入/导出安全**
- **接口安全**

08 8.1 数据公开安全

导入/导出安全

在数据公开阶段，特别是在数据导入导出过程中，面临着多种安全威胁。这些威胁包括数据泄露、中间人攻击、敏感信息未加密传输、数据篡改以及 API 安全漏洞等。

防护措施：

- 采用共享访问控制策略，确保只有经过授权的用户或系统才能访问特定的数据或资源；
- 采用多因素认证（MFA）机制，以增强用户身份的验证强度，防止未授权访问；
- 在数据传输过程中应用强加密算法，以保护数据不被未授权的第三方读取；
- 在必要时对敏感数据进行脱敏处理，例如使用数据掩码、伪匿名化或数据伪装技术，确保在数据导入导出过程中个人隐私和敏感信息不会被泄露；
- 建立全面的数据安全审计系统，记录和监控所有数据访问和修改活动，以便在发生安全事件时能够快速检测、响应和追溯。

08 8.1 数据公开安全

接口安全

在数据公开阶段，用来获取数据最常见的方式之一是使用数据接口，所以数据接口也成为了攻击者重点关注的对象，因为一旦数据接口出现问题，就会导致数据在通过数据接口时发生数据泄露等风险。

防护措施：

- 数据接口安全阶段的技术检测，需要使用技术工具对数据接口的调用进行接口鉴权和接口访问控制，以确保所有人对数据接口的访问与调用都是合法的、符合标准的；
- 对数据接口传输的内容应用隐私计算技术，允许数据使用者在保护隐私的同时充分利用数据的价值；
- 使用加密和脱敏技术能够进一步确保接口调用时的数据完整性、机密性和隐私安全。

第3章 数据安全防护架构

本讲内容概要：

06 第六节—数据传输安全

07 第七节—数据提供安全

08 第八节—数据公开安全

09 第九节—数据销毁安全

09 9.1 数据销毁安全

数据销毁安全是指通过制定数据销毁机制，实现有效的数据销毁管控，防止因对存储介质中的数据进行恢复而导致的数据泄露风险。为了满足合规要求及组织机构本身的业务发展需求，组织机构需要对数据进行销毁处理。

在数据销毁环节，风险主要来自于数据销毁的不彻底性。数据销毁处理要求针对数据的内容进行清除和净化，以确保攻击者无法通过存储介质中的数据内容进行恶意恢复，而造成严重的敏感信息泄露问题。

通常数据销毁安全有以下项：

- **安全销毁**

09 9.1 安全销毁

安全销毁

数据销毁安全是指在监管业务和服务涉及的系统及设备中清除数据时，通过建立针对数据的删除、销毁、净化机制，防止数据被恢复而采取的一系列防控措施。

- 数据安全销毁技术：包含本地数据销毁技术和网络数据销毁技术。
  - 本地数据销毁可使用数据覆写，即将非敏感数据写入以前存有敏感数据的存储位置，以达到清除数据的目的。
  - 网络数据销毁技术又分为基于密钥销毁的数据不可用销毁方式和基于时间过期机制的数据自销毁方式。
- 介质安全销毁技术：对存储介质如闪存盘，磁盘，磁带，光盘等进行物理销毁，确保数据无法复原。主要是通过物理，化学的方式直接销毁存储介质。
  - 物理销毁方法可分为消磁，捣碎，焚毁等方法。
  - 化学销毁方法主要是滴盐酸法。

谢谢！